

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

REMARKS/ARGUMENTS

The Examiner rejected claims 1-43 as anticipated (35 U.S.C. §102(e)) by Elliot (U.S. Pub. No. 2004/0162137). Applicants traverse for the following reasons.

Claims 1, 18, and 27 concern enabling access to data in a storage medium within one of a plurality of storage cartridges capable of being mounted into a interface device, and require providing an association of at least one coding key to a plurality of storage cartridges; determining one coding key associated with one target storage cartridge, wherein the coding key is capable of being used to access data in the storage medium within the target storage cartridge; and encrypting the determined coding key, wherein the coding key is decrypted to use to decode and code data stored in the storage medium.

Applicants amended claims 1 and 27 to clarify antecedent basis of the plurality of storage devices. Applicants request entry of this amendment because it does not necessitate further searching.

Applicants amended independent claim 18 to include a requirement found in independent claims 1 and 27 concerning the "providing" limitation. Applicants submit that adding this requirement already found in independent claims 1 and 27 should be entered because it does not necessitate further searching because the added requirement is already present in the independent claims in the different claim formats.

In the Response to Arguments, the Examiner cited the unique ID of the hard drive and encryption keys that the server utilizes to encrypt the downloaded game software. (Final Office Action, pg. 8; Elliot, paras. 168, 184). The video game system decrypts the received game and stores the game in encrypted form on the hard drive 206. (Elliot, para. 168) A media engine uses an encryption processing to encrypt and decrypt data, and uses a security key that is stored in a hard disk drive in encrypted form to be later decrypted. (Elliot, paras. 189, 190).

The claims require an association of a coding key to a plurality of storage cartridges. Nowhere does the above discussed Elliot disclose this requirement. Elliot discusses how a drive ID is used to encrypt software sent to the video game system. However, this hard drive is associated with just one drive device, and not a plurality of storage cartridges as claimed. Elliot further discusses a security code to encrypt games stored on the hard disk drive. Again, this mentions one code to store games on a single drive and does not disclose one coding key associated with a plurality of storage cartridges.

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

Further, nowhere does the cited Elliot anywhere disclose encrypting a determined coding key associated with a plurality of storage devices so that the decrypted coding key is used to decode and code data in the storage medium. The cited Elliot discusses a security code that is stored in the hard disk driver 206 in encrypted form to be later decrypted by the encryption processing engine 406. (Elliot, para. 189) The encryption processing engine decrypts data on the fly. (Elliot, para. 191)

Although the cited Elliot discusses a security code that is encrypted and decrypted and used by an encryption processing engine, nowhere does the cited Elliot disclose the claim requirement that the security code comprises a coding key associated with a plurality of storage cartridges that are capable of being mounted into an interface drive. Instead, the cited security code of Elliot is used by the encryption processing engine 406 that encrypts data on the video game system disk drive.

The additional sections of Elliot the Examiner cited in the Response to Arguments, including paragraphs 225, 251, 264, and 265, nowhere disclose the combination of claim requirements of a coding key that is associated with a plurality of storage cartridges and used to access data in a target storage cartridge, where the coding key is encrypted and decrypted to decode and code data in the storage cartridge.

The Examiner further cited paragraphs 5, 15-18, 80, 109, 160, 164-168, 176-178, 183, and 184 of Elliot as disclosing the requirements of these claims. (Final Office Action, pg. 2) Applicants traverse.

Paragraph 5 discusses counterfeiting of video game cartridges for video game systems. Paragraphs 15-18 discuss how an expansion device may be attached to a video game console, where the expansion device has a storage device and unique ID associated with the storage device. The expansion device requests a server to download a video game. The expansion device and server communicate using encryption keys.

Cited paragraph 18 discusses how the server utilizes the unique ID of the expansion device hard drive and encryption keys to encrypt a downloaded game. The server also identifies to a disk controller in an expansion device the partitions a particular game may access.

Cited paragraphs 168 and 184 mention that the expansion device sends the unique ID of its hard drive encrypted to the server. The server uses the unique ID to encrypt the video game. The video game system receives the game, and the game is decrypted and executed and stored in encrypted form on the hard drive.

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

The claims concern enabling access to storage cartridges capable of being mounted to an interface device. The cited Elliot discusses a unique ID associated with a hard disk drive in an expansion device. There is no disclosure in the cited Elliot that the interface of the hard disk drive in the expansion device may mount multiple storage cartridges. Elliot discusses game cartridges, but the cited unique ID sent to the server and used to encrypt the video game is not associated with the game cartridges, but instead is the ID of the disk drive of the expansion device attached to the game console. Thus, the cited keys and codes of Elliot are not associated with a plurality of storage cartridges.

The claims further require that the coding key is capable of being used to access data in the storage medium within the target storage cartridge with which the coding key is associated. In the cited Elliot, the unique ID of the expansion device hard disk drive is used by the server to transmit a video game to the expansion device. However, there is no disclosure in the cited Elliot that this same cited unique ID is also used to access data in the storage medium within the target storage cartridge as claimed. The cited paragraph 168 mentions that the game is stored in encrypted form on the hard drive 206. However, the cited Elliot does not disclose that the unique ID is also used to access data within the storage media as claim. The cited Elliot does not disclose the use of the unique ID for encryption other than encrypting the video game to communicate from the server to the expansion device.

Accordingly, for the above reasons, Applicants submit that the independent claims 1, 18, and 27 are patentable over the cited art because the cited Elliot does not disclose all the claim requirements.

Claims 2-9, 19-22, and 28-35 are patentable over the cited art because they depend from one of claims 1, 18, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, the below discussed independent claims provide additional grounds of patentability over the cited art.

Claims 5 and 31 depend from claims 1 and 27 and further require that the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge. The Examiner cited the same above cited paragraphs of Elliot as disclosing the additional requirements of these claims. (Final Office Action, pgs. 3-4) Applicants traverse.

The cited Elliot discusses how a server uses a unique ID of an expansion device disk drive to send an encrypted game to the expansion device. Nowhere does the cited Elliot disclose

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

that the unique ID comprises a seed value used to generate an additional key. Applicants request that the Examiner specifically identify where Elliot discloses that the unique ID associated with the expansion device disk drive may be used as a seed value used to generate an additional key used to directly decode and encode data in the cartridge.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 8 and 34 depend from claims 6 and 32 and provide details of how the coding key is encrypted with a first key and that another key used to decrypt a second key capable of decrypting the coding key encrypted with the first key. The Examiner cited the same above cited paragraphs of Elliot as disclosing the additional requirements of these claims. (Final Office Action, pg. 4) Applicants traverse.

The cited Elliot mentions that the unique ID may be encrypted and sent to the server. However, nowhere does the cited Elliot anywhere disclose encrypting and transmitting a second key used to decrypt the unique ID. Further, Elliot also mentions the security code that is decrypted and encrypted. However, nowhere does the cited Elliot disclose the use of the second, third and fourth keys to decrypt the coding key and data as claimed.

Accordingly, claims 8 and 34 provide additional grounds of patentability over the cited art.

Claims 9 and 35 depend from claims 6 and 32 and provide details of how the coding key is encrypted with a first key, then decrypted by a second key, and then encrypted with a fourth key. The Examiner cited the same above cited paragraphs of Elliot as disclosing the additional requirements of these claims. (Office Action, pg. 5) Applicants traverse.

The cited Elliot mentions that the unique ID may be encrypted and sent to the server. However, nowhere does the cited Elliot anywhere disclose encrypting the unique ID with a first key, decrypting with a second and then encrypting with a third key that may be decrypted by a fourth key. Further, Elliot also mentions the security code that is decrypted and encrypted in a hard disk drive. However, nowhere does the cited Elliot disclose the use of the second, third and fourth keys to decrypt the coding key and data as claimed.

Accordingly, claims 9 and 35 provide additional grounds of patentability over the cited art.

Independent claims 10, 23, and 36 concern accessing data in a removable storage cartridge including a storage medium, and require: receiving an encrypted coding key from a

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

host system; decrypting the encrypted coding key; using the coding key to encode data to write to the storage medium; and using the coding key to decode data written to the storage medium. The Examiner cited the same above cited paragraphs of Elliot as disclosing the additional requirements of these claims. (Final Office Action, pg. 5) Applicants traverse.

As discussed, the cited Elliot discusses how the expansion device sends an encrypted unique ID associated with a hard drive to the server, and the server encrypts and sends a video game back. Nowhere does the cited Elliot disclose encrypting an encrypted coded key received from a host to encode and decode data written to a storage medium. Instead, the cited Elliot discusses the server decrypting an encrypted unique ID to use to encrypt a video game. However, the Examiner has not cited any part of Elliot that discloses that the decrypted unique ID is used to encode and decode data in the storage medium as claimed.

Moreover, the cited Elliot concerns a unique ID that is used to encrypt data for a hard disk drive, not a removable storage cartridge as claimed.

As discussed, Elliot also discusses separately a security code that is stored in a hard disk drive and encrypted and later decrypted for use by the encryption processing engine. (Elliot, para. 189). However, nowhere does Elliot disclose that this encrypted coding key is received from a host system and used to encode and decode data in a removable cartridge storage medium.

Accordingly, for the above reasons, Applicants submit that the independent claims 10, 23, and 36 are patentable over the cited art because the cited Elliot does not disclose all the claim requirements.

Claims 11-17, 24-26, and 37-43 are patentable over the cited art because they depend from claims 10, 23, and 36, which are patentable over the cited art for the reasons discussed above. Moreover, the dependent claims provide additional details about how the coding key may be encrypted and decrypted. The cited Elliot does not disclose the additional requirements of the dependent claims with respect to how the server and expansion device communicate the unique ID that the server uses to encrypt the video game being sent. Accordingly, these dependent claims provide further grounds of patentability over the cited art.

Amdt. dated July 29, 2005
Reply to Office action of June 6, 2005

Serial No. 09/977,159
Docket No. TUC920010022US1
Firm No. 0018.0092

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-43 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: July 29, 2005

By: 

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984